

A hand is shown in the upper left corner, having just tossed a coin into the air. The coin is captured mid-air above the buckets. Three galvanized metal buckets are arranged in a row. The leftmost bucket is labeled 'LOW', the middle one 'MEDIUM', and the rightmost one 'HIGH'. Numerous coins are scattered on the surface in front of the buckets, with a higher concentration in front of the 'HIGH' bucket. The background is plain white.

The Fallacy of Quantifying Risk

David E. Frick, Ph.D.

Nearly every article you see in industry and within the DoD literature on the topic of “risk management” demonstrates, advocates, or aggrandizes the attempt to quantify risk. One might think that if risk management was truly a science and uncertainty could be systematically quantified in some manner, then the maturity of the profession of project or program management, as measured by the number of projects or programs that meet cost, schedule, and performance goals, would increase over time. Alas, the profession is not able to make this claim.

A recent article in a professional publication was no exception and prompted this response. The author suggested that a key to risk analysis was “choosing the right technique” of quantifying risk. The weakness in this argument stems not from the assertion that one approach may be superior to another, but rather from the basic assumption

Frick is a 35-year veteran of the Department of Defense. He is currently an acquisition professional and active risk practitioner.

that risk (arising from uncertainty) in every situation can, in fact, be quantified.

One profession-wide barrier to a more meaningful discussion on this topic is our collective looseness in the use of language. The lack of a common taxonomy serves to exacerbate this barrier. In this same article, the terms “risk analysis” and “assessment of uncertainty” appeared to represent the same concept. They are two distinct concepts. The word “risk” is the feeble attempt by humans to define the ephemeral abstraction of uncertainty as a tangible term. “Risk,” as we commonly use the term, is inherently unquantifiable.

Quantitative techniques rely on empirical data, or at least highly defensible estimates. When you discuss the uncertainty of the weather or solar flares, the historical data are sufficient to make assertions that do not cause statisticians to cringe. When you discuss the uncertainty surrounding a first-time, never-to-be-repeated project or a major systems acquisition (MSA) designed to rely on technology that has not reached maturity, germane historical data seldom exist. One is truly in a state of not knowing what is not known. Estimates presented to the Milestone Decision Authority (MDA), based on experience and judgment, do have their value—but the inexactness of most quantitative assessments of the true state of uncertainty surrounding programs makes predictions based on these analyses no more useful than flipping a coin. Estimates may be all we have, but we should not impute to them some characteristic of certainty that does not exist.

Other disciplines, such as the insurance industry and medicine, use the same term to represent concepts dissimilar to DoD’s use of the term. The differences are subtle yet critical, and these subtle differences confound us.

In the insurance industry, years, decades, and centuries of historical data give actuaries high confidence in making generalizations of aggregates. While no insurance company can declare honestly that any given man, born in 1955, non-smoker in good health, will live another 23.26 years, it can declare with the utmost certainty that on average, all men in this category will. These actuaries bet their companies’ financial health on the ability to accurately interpret a large amount of historical data.

In medicine—in the United States, anyway—drug companies spend billions of dollars annually to gather data. Test populations only number in the hundreds and sometimes the thousands, but thanks to the beauty of the law of truly large numbers—with a sample size large enough, any outrageous thing is likely to happen—we can be confident that properly conducted studies will, in fact, uncover almost all of the unintended consequences of a drug’s effects. However, in DoD acquisitions, we cannot be as confident for a very simple reason—relevant historical data for first time, never to be repeated programs do not exist. Yes, we have ample data on programs, in general, but each program is unique, will face unique challenges, and

will involve a unique set of people. The dissimilarities vastly outnumber the similarities.

Pronouncements that risk registers, quantitative techniques, or milestone reviews “reduce the number of risks” demonstrate another fundamental misunderstanding of uncertainty. First, in the current parlance and practice, the term risk “should” be associated with numeric value—a composite of the probability that a specific threat will manifest and the impact of that manifestation. In program management, we are concerned with the impact on cost, schedule, or performance. We all recognize the equation $\text{Risk} = \text{Probability} \times \text{Impact}$ —or some pair of the terms potential, likelihood, damage, effect, and consequences. Probability is a number (0.0 to 1.0). Impact is usually visualized as something that can be measured, e.g., dollars (cost); hours, days, or weeks (schedule); or customer satisfaction, quality, speed, durability, mean time between failures (performance). Therefore, “risk” should be defined in terms of one or more specific units.

For example, the result of some event might have an impact of \$10,000 plus 4 days schedule slip plus a 10 percent reduction in system performance. Instead, in DoD, we choose to place probability in one of never more than five, overly simplistic buckets—very low (1), low (2), medium (3), high (4), and very high (5); then we do the same to impact. The product of these assignments is a number in the range of 1 to 25. Then, we arbitrarily slice this range into three sections and name them low, medium, or high. Talk about excessive aggregation! Can you imagine an insurance company only offering three premium levels to a population as diverse as ours? Such an approach would not endanger the insurance company, if its client base was large enough, but I suspect that discriminating consumers, at least those in the low risk categories, would shop elsewhere.

Second, while “risk mitigation” may reduce the total number of threats (by reducing probability or impact of a specific threat to zero), what the practitioner usually means is that the value of the risk for a specific post-mitigation threat is so inconsequential that it no longer merits an expenditure of brainpower. Nonetheless, the specific threat still exists and even the highly improbable event does occasionally manifest. Nassim Taleb refers to this as the “black swan” event.

Third, while eliminating a single threat from consideration may have value, if you consider the near infinite number of threats that may affect a program but are not being considered because they are so remote in possibility or simply not known or knowable, suggesting that a specific program faces no more than 10, 100, or even 1,000 “risks” is naïveté.

In the “identification phase” of “risk analysis” (better named threat identification), practitioners are wont to stop identifying threats at some arbitrary point, usually the number of lines that fit on the risk slide in some PowerPoint presentation. Admittedly, there is a point at which the cost of committing threats



The inexactness of most quantitative assessments of the true state of uncertainty surrounding programs makes predictions based on these analyses no more useful than flipping a coin.

to paper exceeds prudence. A human extinction-level event (such as a massive meteor strike) would likely have devastating consequences on your project, program, or MDA. This threat always exists, but expending time and effort thinking about it (or reporting it to the MDA) would probably not be prudent. The question is how many low-probability/high-impact threats are not being considered simply because some risk analyst ran out of lines in the risk register or simply failed to identify them?

Furthermore, while uncertainty comprises the totality of possible good things (opportunities) and bad things (threats), invariably, most risk management practitioners only consider the bad things. I laud DoD and the Project Management Institute (PMI) for stressing this point by stating in the *Risk Management Guide to DoD Acquisition*, 6th Edition, and the PMBOK Guide—Fourth Edition, that the objectives of risk management are to increase the probability and impact of positive events and decrease the probability and impact of negative impacts. Nonetheless, in the common parlance, risk continues to be synonymous with the consequences of the negative. For myriad reasons, the discussion of potential opportunities tends to get short shrift.

The issue becomes more absurd in risk averse organizations. There is nothing objectionable to an organization being risk averse, especially in response to the contemporaneous propensity of Congress, but when the analyst allows a conservative trend to influence the analysis of a project's or program's potential success, the program management profession is harmed. Big risk-big reward may be a good cliché for the mission statement, but the culture of the organization will more strongly influence the final risk assessment than the printed strategic plan. High-impact threats are often hidden or ignored. Estimates are viewed through the lens of the best case scenario. The MDA then makes decisions based on information that is incomplete, so more programs fail than anticipated.

Risk handling and risk mitigation, also terms without precise universally-accepted definitions, are terms commonly thrown about by program management practitioners to justify removing a specific identified threat from the few listed in the risk register. Both PMI and DoD identify four risk mitigation techniques: avoiding (eliminating the threat or consequence), reducing (the probability or consequences of the threat manifesting), transferring (this method is a bit nebulous, but view it as making the threat someone else's problem, e.g., insurance), or assuming (the risk).

Consider, instead, the proposition that from the perspective of the major program, there exist only two categories of action to handle or manage risk:

- Reduce the composite risk index. This means taking some action within the limits of available knowledge and resources that decreases the probability of a threat manifesting (hopefully to zero) or reducing its impact (again, hopefully to zero).
- Assuming the risk, when probability and impact are both greater than zero.

All actions under the rubric of "risk mitigation" or risk handling fall in this first category. Risk avoidance, e.g., deciding not to start a program, is one manner of reducing the probability of the threat to zero. Risk transfer, e.g., insurance, reduces the impact from the perspective of the program to near zero. To stress the point, risk mitigation "always" has a cost, e.g., expenditure of resources or the ephemeral opportunity costs. Risk mitigation becomes a recursive exercise in cost-benefit analyses. In the end, when all efforts at mitigating risk have been exhausted or evaluated as too costly for the potential benefit and the probability and impact of a specific threat is still greater than zero, the only recourse left is the second category—to assume the risk. Assuming risk should not be considered bad leadership. On the contrary, history is replete with examples of commanders assuming great risk (usually arising from lack of information about the enemy), yet achieving great outcomes.

Attempts at quantifying risk are not, in and of themselves, objectionable. Prudence demands that program management practitioners quantify, to the greatest extent practicable, and prioritize known threats so that limited resources can be applied in a thoughtful manner to reduce the component probabilities and impacts. On the other hand, the practice of stating to some level of surety that, based on some esoteric risk analysis, program risk is low, medium, or high, is damaging to the program management profession. The unexpected, harmful "black swan" event can suggest to those not well schooled in risk management/risk analysis that the

offered analysis was incomplete, incompetent, faulty, or dishonest—not good for the program management profession and replete with consequences, e.g., Nunn-McCurdy reviews.

Practitioners would be much better served to be more complete in acknowledging and reporting the complete state of uncertainty in a project. The output of a complete risk analysis should include:

- The number of threats identified in threat identification
- The number of identified threats for which either probability or impact can or have been reduced to zero
- The number of identified threats for which the composite risk cannot be reduced to zero within current resource constraints and must be “assumed”
- An enumeration of the identified threats for which the organization has no historical experience
- The magnitude of the unknown-unknowns. Of course, this number cannot be quantified, but an honest, subjective assessment is much more valuable to the MDA than is silence. An assessment of project success. Again, this is a highly subjective assertion. Be honest. An honest, subjective assessment is much more useful to the MDA than the typical, overly optimistic, agenda-driven pronouncements.

Big risk-big reward may be a good cliché for the mission statement, but the culture of the organization will more strongly influence the final risk assessment than the printed strategic plan.



Human nature is replete with cognitive biases. Multiple studies have shown how estimates are subject to the confounding influence of expectation bias. A can-do attitude is a great characteristic, unless it blinds the program manager to the obvious truth. Take a step back and have the courage to admit you don't know what you don't know. &

The author can be reached at david.frick@dodiis.mil.

Defense AT&L has become an online-only magazine for individual subscribers.

If you would like to start or continue a subscription with **Defense AT&L**, you must register a valid e-mail address in our LISTSERV

All Readers: Please subscribe or resubscribe so you will not miss out on receiving future publications.

- Send an e-mail to datlonline@dau.mil, giving the e-mail address you want us to use to notify you when a new issue is posted.
- Please type “Add to LISTSERV” in the subject line.
- Please also use this address to notify us if you change your e-mail address.

